Are You Ready to PK-Enable?

By Rebecca Nielsen and Kenya Spinks

Wouldn't it be so much simpler if Department of Defense (DoD) personnel had to remember only one simple Personal Identification Number (PIN) to carry out their daily responsibilities, no matter where they worked or traveled in an official capacity? As a result of new technology, this possibility will soon become a reality because all DoD members will rely on digital credentials to authenticate (i.e., verify their identity) to their private Web servers and applications, in lieu of conventional usernames and passwords.

Two memos from the Assistant Secretary of Defense (ASD), dated May 17, 2001[1] and May 21, 2002[2], set forth the importance of Public Key Infrastructure (PKI) in the DoD Information Assurance (IA) technical strategy. The earlier memo, "Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the DoD," states, "e-mail in all operating environments and Web applications in unclassified environments shall be PK-enabled." The later memo, "Public Key Infrastructure (PKI) Policy Update" provided implementation dates of October 2003. However, the Department of the Navy Chief Information Officer (DON CIO) is aware that not all Navy Marine Corps Intranet (NMCI) eligible sites will have transitioned by the October 2003 deadline, and released a Naval message[3] granting the Department a six-month grace period. The Department's new implementation date for meeting the three PKE milestones, identified in the May 21, 2002 memo, is April 1, 2004, as shown in the chart below.

The plan is to meet the milestones via enterprise solutions within the DON. For example, the rollout of the NMCI includes the public key-enabled Microsoft Outlook e-mail client and Microsoft Windows 2000, which are capable of certificate-based logon. Sites that have already transitioned to NMCI should be on their way toward meeting the first two milestones.

Existing October 2002 Requirement	Adjusted Milestone Date
Milestone 1: Ensure all electronic mail (e-mail) sent within DoD is digitally signed	April 2004
Milestone 2: PK-enable DoD unclassified networks for hardware token, certificate-based access control	April 2004
Milestone 3: PK-enable Web applications in unclassified environments	April 2004

The Navy Marine Corps Portal (NMCP) will support applications requiring PK-enabling. If the application requires only authentication, then integrating the application with the NMCP single sign on (SSO) solution meets the PK-enabling requirement. This article focuses on how to meet the third milestone, PK-enabling Web applications in unclassified environments.

What Is PK-Enabling?

PK-enabling is the process of using Public Key Infrastructure to provide solutions for some IA requirements. PKI itself is a framework established to issue, maintain and revoke public key certificates.[4] A certificate is a digital representation of information that at least:

√ identifies the certification authority issuing it
√ identifies or names its subscriber
√ contains the subscriber's public key
√ identifies its operational period
√ is digitally signed by the certification authority issuing it[5]

The DoD has established a PKI to issue certificates to all DoD military and civilian employees and to other individuals who work full-time on-site at DoD facilities. DoD PKI certificates are issued primarily on Common Access Cards (CAC). Eligible personnel, known as subscribers to the PKI, who receive their CAC, hold three digital credentials: an identity certificate, an e-mail signing certificate and an e-mail encryption certificate.

PK-enabling provides applications with the capability to rely on digital certificates, either in lieu of existing technologies such as usernames and passwords or to enhance functionality such as incorporating digital signatures. Because PKI is based on cryptography, PK-enabling can also provide encryption services such as creating an encrypted channel through an untrusted network or encrypting a file or message so that only the intended recipient can read it.

PK-enabling not only enhances the overall security of the application, but also provides user and administrator benefits by reducing the requirement for both individual and application password management. Users will no longer be required to remember usernames and passwords for each system they are authorized to access. Instead, users need only remember the single password that unlocks the private key on their CAC. Administrators, while still required to manage who is authorized to access system resources, can map access rights to certificate identities and do not have to develop methods for transmitting initial passwords or managing password reset requests.

How to PK-Enable Web Applications

The primary requirement for PK-enabling Web-based applications is to authenticate users based on their digital certificate and associated private key. Certificate-based authentication consists of three steps: (1) establishing an encrypted communication channel, (2) validating the subscriber's certificate, and (3) performing a challenge-response between the server and the client to ensure that the user is the subscriber named in the certificate.

• Step 1: Establishing an encrypted communication channel. This step uses a protocol known as Secure Sockets Layer (SSL), or its successor, Transport Layer Security (TLS). This protocol requires that the application server send its public key certificate to the client. The client then generates the shared secret that will be used for the encrypted channel, encrypts it with the public key in the server's certificate and sends it to the server. The server's private key is required to decrypt the shared secret, so the client and server have now exchanged a key that is used for all further communications.

• Step 2: Validating the subscriber's certificate. After an encrypted

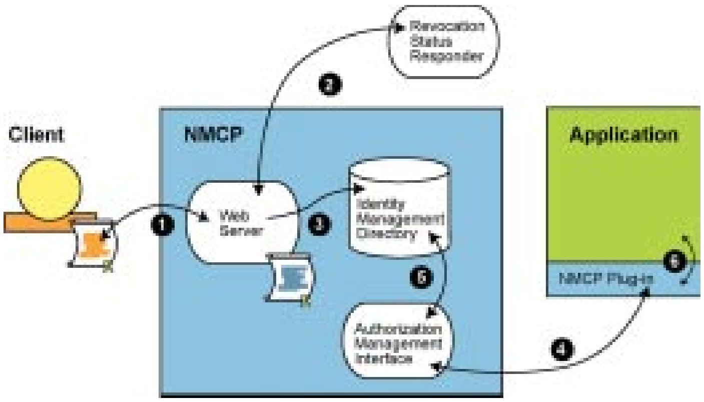
Revocation Status Responder
2
Client
NMCP
Application
Web Server
1
3
Identity Management Directory
6
5
NMCP Plug-in
Authorization Management Interface
4

Figure 1.
Integrating an Application with NMCP

√ NMCP Web server performs certificate-based authentication.

√ NMCP communicates with revocation status responder to ensure user's certificate has not been revoked.

√ NMCP Web server provides identity of user to NMCP identity management directory.

√ After the user has requested access to an application (not shown), the application communicates with the NMCP authorization management interface to determine the user's identity and authorizations.

√ NMCP authorization management interface retrieves identity and authorization information from NMCP identity management directory.

√ NMCP authorization management interface provides user identity and authorization information to application via the NMCP plug-in.

channel has been established, the client sends the subscriber's certificate to the server. The server validates that the certificate was issued by a PKI that the server trusts, that the certificate has not expired and that the certificate has not been revoked. To support PK-enabling, the NMCI office is establishing responders at each Network Operations Center that can respond to requests from applications regarding the revocation status of certificates.

• Step 3: Performing a challenge-response between the server and the client. Because certificates are public, the server must now establish that the user attempting access is actually the subscriber named in the certificate. The server then sends a challenge to the client. The client must digitally sign the challenge using the private key that exists only on the CAC issued to the subscriber and return the signed challenge to the server. The server can use the subscriber's certificate to verify the signature on the challenge.

If these three steps are successful, the server can trust that the identity of the user is the same as the identity stated in the certificate and can then map that identity to authorizations.

NMCP — The Pathway to Single Sign On

The Department of the Navy intends to PK-enable at the enterprise portal level rather than requiring every application to be enabled. The DON CIO "NMCP Policy Guidance Memorandum"[6] conveys the DON's approach to establish a framework for organizing, managing and accessing departmental information through an integrated portal structure. The DON CIO is responsible for establishing a set of standards for the portal that focuses on quality assurance, quality of service, data standardization, metadata management, interoperability and enterprise-level information resource management.

The NMCP is a Web-based, user-customizable service that provides single sign on to all Web services using certificate-based authentication. The NMCP will pass authorization tokens extracting unique identifiers from the identity certificate to various Web Services behind the portal. The Department affirms that enabling at the portal level is not only feasible, but also cost effective. This is a benefit to each application developer and will not require individual applications to be enabled.

Applications that have already been PK-enabled should experience a more effective interface to the NMCP. In the future, these same authorization tokens will contain specific role-based attributes, allowing only those users who have the need-to-know with access to those enabled Web applications. Those Web Services requesting access from the NMCP must have their services registered in the NMCP service registries.

The NMCP will further support functional and organizational collaboration across the DON and promote DON-wide process engineering. The end user and organizational commands will be able to subscribe to desired services, tailor the view provided and have these services provided at each logon to the enterprise portal. Figure 1 illustrates the future NMCP architecture.

Summary

The Department of the Navy is taking aggressive steps to meet DoD PK-enabling requirements primarily through the strategic use of the NMCI and the NMCP. Developers of applications that have been identified by the Functional Area Manager (FAM) as either approved applications or approved with restrictions should coordinate with their Functional Area Manager to integrate their Web-based applications with the NMCP. Some organizations may own applications with constraints that prevent them from fulfilling these requirements. These organizations should contact their appropriate chain of command for guidance. For more information regarding the NMCP, contact David.O.Rose@navy.mil.

References:

1. Assistant Secretary of Defense (ASD) Command, Control, Communications and Intelligence (C3I/CIO) Memorandum, "Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense (DoD)" of May 17, 2001.

2. Assistant Secretary of Defense (ASD) Command, Control, Communications and Intelligence (C3I) Memorandum, "Public Key Infrastructure (PKI) Policy Update" of May 21, 2002.

3. DON CIO Washington 292338Z SEP 03.

4. X.509 Certificate Policy for the U. S. Department of Defense.

5. American Bar Association. Digital Signature Guidelines. August 1, 1996.

6. Department of the Navy Chief Information Office Memorandum, "Navy Marine Corps Portal (NMCP) Policy" of February 28, 2003.

Rebecca Nielsen and Kenya Spinks support the DON CIO Information Assurance Team.